REMARKS / ARGUMENTS

This application is believed to be in condition for allowance because the claims are non-obvious and patentable over the cited references. The following paragraphs provide the justification for this belief. In view of the following reasoning for allowance, the applicants hereby respectfully request further examination and reconsideration of the subject patent application.

1.0 Rejections under 35 U.S.C. §103(a):

In the Office Action of December 3, 2004, claims 1-23 were rejected under 35 U.S.C. §103(a) as being unpatentable over Brown, et al. ("***Brown***," U.S. Patent No. 5,887,133) in view of Schneider, et al. ("***Schneider***," U.S. Patent No. 6,408,336).

In order to deem the Applicant's claimed invention unpatentable under 35 U.S.C. §103(a), a prima facie showing of obviousness must be made. However, as fully explained by the M.P.E.P. Section 706.02(j), to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference ***or to combine reference teachings***. Second, ***there must be a reasonable expectation of success***. Finally, ***the prior art reference (or references when combined) must teach or suggest all the claim limitations***.

Further, in order to make a prima facie showing of obviousness under 35 U.S.C. 103(a), ***all*** of the claimed elements of an Applicant's invention must be considered, ***especially when they are missing from the prior art. If a claimed element is not taught in the prior art and has advantages not appreciated by the prior art, then no prima facie case of obviousness exists***. The Federal Circuit court has stated that it was error not to distinguish claims over a combination of prior art references where a

material limitation in the claimed system and its purpose was not taught therein (*In Re Fine*, 837 F.2d 107, 5 USPQ2d 1596 (Fed. Cir. 1988)).

1.1 Rejection of Claims 1-12:

Independent claim 1 was rejected under 35 U.S.C. §103(a) based on the rationale that ***Brown***, in view of ***Schneider***, teaches the Applicants claimed "system for remotely controlling a security state for each frame" of a web page having multiple frames. However, the Applicants respectively suggest that independent claim 1 is patentably distinct from the combination of the cited references in view of the discussion provided below.

Specifically, the Office Action rejected independent claim 1 under 35 U.S.C. §103(a) based on the rationale that ***Brown*** discloses the invention as described and claimed by the applicant, but that "insecure communications in a security setting are considered in the art to be undesirable, Brown does not consider security considerations." The Office Action then cites the ***Schneider*** reference as disclosing "the raising of different trust levels in a group of objects to the highest trust level being used (see column 10, lines 12-19)."

However, in contrast to the position advanced by the Office Action, the applicants contend that the ***Brown*** reference in view of the ***Schneider*** reference fails to teach the limitations of the applicant's claimed invention, and respectfully suggest that the Office Action has incorrectly characterized both the ***Brown*** and ***Schneider*** references in view of the applicants' claimed invention, and has also incorrectly characterized the suggested capabilities of the hypothetical system resulting from the proposed combination of the ***Brown*** and ***Schneider*** references.

In particular, the Office Action first suggests that "Brown discloses a document generator wherein undesired portions (frames) in a document are automatically located

by a system located in the Internet (see column 3 line 54) based upon a determination by a proxy server (see column 3, line 66 to column 4, line 6)." Next, the Office Action suggests that this determination "is further based upon the layout of the intermediate document (see column 4, lines 42-49), which is then delivered to the user's controller (see column 4, lines 53-57), where it can be further updated based upon the user profile."

The ***Brown*** reference is clear regarding the capability to "automatically" determine the location of "undesired portions (frames) in a document..." In particular, ***Brown*** explains that this determination is made by parsing the text or html code of the document to locate particular predefined keywords or addresses, such as the term "<!-AdSpace->" or the network address of a particular known ad server (see for example, col. 8, line 37 to col. 9, line 10). Once such keywords or addresses have been identified, ***Brown*** provides an alternate content of the same size as the original content to replace the "undesirable" content.

In addition, ***Schneider*** is also clear on the security features provided by the system disclosed in the ***Schneider*** reference. In particular, ***Schneider*** explains that a "***scalable access filter***... is used... to control access... to information..." "Each user belongs to one or more user groups and each information resource belongs to one or more information sets. Access is permitted or denied according to [a set] of access policies which define access in terms of the user groups and information sets..." "Access is further permitted only if the trust levels of a mode of identification of the user and of the path in the network by which the access is made are sufficient for the sensitivity level of the information resource. If necessary, the access filter automatically encrypts the request with an encryption method whose trust level is sufficient" (see Abstract and col. 8, line 34, through col. 10, line 34).

In other words, ***Schneider*** discloses a system wherein the access rights of particular users to particular sets of information are first verified, followed by a

verification of the security level ("trust level") of the path by which the user is attempting to access that information. Clearly, the verification of both user security levels and the security of the path by with the user is attempting to access that data is a concept that is practiced by a large number of references. However, this particular feature for verifying user security and access path security has no bearing on the invention being disclosed and claimed by the applicants.

As noted above, ***Brown*** operates to parse documents to identify particular predefined keywords or addresses that have been labeled as being objectionable by the creator of a list of objectionable content. Consequently, when combined with the ***Schneider*** reference, it should be clear that the resulting hypothetical system is one in which documents having objectionable content are cleaned up by replacing that objectionable content and then provided only to those users having a sufficient security level to be allowed to access that cleaned up content via a network channel also having a sufficient security level. Clearly, such a system provides no capability whatsoever for determining the individual security states of individual frames making up a single web page, nor of ensuring that each frame maintains the same security state by reloading frames having different security states with frames having the same security state, as disclosed and claimed by the applicants.

In fact, as noted above, the Office Action suggests that the ***Schneider*** reference discloses "the ***raising of different trust levels in a group of objects to the highest trust level*** being used (see column 10, lines 12-19)" (emphasis added). However, the applicants respectfully suggest that this position advanced by Office Action is in error, and is not supported by the cited text.

Specifically, column 10, lines 12-19 of the ***Schneider*** recites the following language: "the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through

the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks." By itself, the cited text is very limited, and seems merely to suggest that various ***data access methods*** and ***network paths*** used to access ***particular data*** can have ***different security levels***. Consequently, the text of the ***Schneider*** reference does ***not*** seem to be in agreement with the suggestion by the Office Action that the ***trust level of each object in a set of objects is raised*** to the highest level being used.

However, when read in the context of the surrounding text, the meaning of the cited text becomes clear. In particular, col. 10, lines 6-34 of the ***Schneider*** reference explain that:

> "The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. ***The trust level of a request has a number of components***:
>
> the ***trust level of the identification technique*** used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address.
>
> the ***trust level of the path taken by the access request*** through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks.
>
> if the access request is encrypted, ***the trust level of the encryption technique*** used; the stronger the encryption technique, the higher the trust level.

> "***The trust level of the identification technique and the trust level of the path are each considered separately***. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. ***If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique***. Thus, ***if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level.***" (emphasis added)

The meaning of the cited text should now be clear in view of the broader context of the surrounding disclosure of the ***Schneider*** reference. In particular, ***Schneider*** is clearly explaining that the "trust level" of particular user identification techniques may be different. In addition, ***Schneider*** is also clearly explaining that the trust level of a particular portion of a ***network path*** used in an attempt to access requested data on a network can be varied depending upon the ***encryption level of the data request*** sent across that path. Clearly, checking the "trust level" of a particular identification technique and varying a trust level of a network path as a function of the level of data encryption used on that path, as disclosed by the ***Schneider*** reference does ***not*** disclose that the "trust level of each object in a set of objects is raised to the highest level being used" as suggested by the Office Action.

Further, in view of the preceding discussion, it should also be clear that in contrast to the position advanced by the Office Action, the ***Schneider*** reference fails completely to provide any disclosure or suggestion for determining the various security states of individual frames within a single web page. In addition, it should also be clear that the ***Brown*** reference also fails to disclose such a feature, and in fact, the Office Action has admitted that ***Brown*** does not disclose this feature.

Consequently, the proposed ***Brown / Schneider*** combination ***fails to teach or suggest all the claim limitations***. Therefore, in view of the preceding discussion, the applicants respectfully suggest that no prima facie case of obviousness has been established in accordance with M.P.E.P. Section 706.02(j) and in accordance with the holdings of *In Re Fine*. This lack of a prima facie showing of obviousness means that the rejected claim 1, and thus dependent claims 2-12 are patentable under 35 U.S.C. §103(a). Therefore, the Applicants respectfully traverse the rejection of claims 1-12, and request reconsideration of the rejection of claims 1-12 under 35 U.S.C. §103(a) over ***Brown*** in view of ***Schneider*** in view of the non-obviousness of the language of claim 1. In particular, claim 1 recites the following novel language:

> "In an Internet web page having at least two frames, a system for remotely controlling a security state for each frame comprising:
>
> ***automatically determining a security state of a called Internet web page when a local client computer calls that Internet web page from a remote server computer for inclusion in at least one of the frames***;
>
> ***automatically determining whether the called Internet web page has a security state different from any existing frames which comprise an initial Internet web page on the local client***;
>
> wherein the remote server automatically ***directs the local client to load replacement frames for any existing frames which have a different security state*** than the called Internet web page, with the replacement frames having the same security state as the called Internet web page; and
>
> wherein the local ***client automatically generates a new Internet web page*** comprising the called Internet web page and the replacement frames in response to the direction from the remote server to the local client, and ***wherein all frames of the new Internet web page have the same security state***." (emphasis added)

1.2 Rejection of Claims 13-17:

The Office Action rejected independent claim 13 under 35 U.S.C. §103(a) based on the same rationale as that used for the rejection of independent claim 1, as discussed above, with the additional suggestion that "the web page may vary depending upon the caller (see Brown, column 8, lines 28-36)." However, the Applicants respectively suggest that independent claim 13, which claims "automatically controlling a security state for an Internet web page having at least two frames" is patentably distinct from the combination of the cited references in view the preceding discussion.

Specifically, as noted above, the proposed ***Brown / Schneider*** combination ***fails to teach or suggest all the claim limitations***, including for example, the claimed limitation of "automatically directing the local client computer, via the security state script, ***to load replacement frames having the desired security state for each frame of the Internet web page.***"

Therefore, in view of the preceding discussion, the applicants respectfully suggest that no prima facie case of obviousness has been established in accordance with M.P.E.P. Section 706.02(j) and in accordance with the holdings of *In Re Fine*. This lack of a prima facie showing of obviousness means that the rejected claim 13, and thus dependent claims 14-17 are patentable under 35 U.S.C. §103(a). Therefore, the Applicants respectfully traverse the rejection of claims 13-17, and request reconsideration of the rejection of claims 13-17 under 35 U.S.C. §103(a) over ***Brown*** in view of ***Schneider*** in view of the non-obviousness of the language of claim 13. In particular, claim 13 recites the following novel language:

> "Automatically controlling a security state for an Internet web page having at least two frames in accordance with the following acts:
>
> ***providing a remote server computer in communication with the Internet, the remote server hosting a dynamic web page script***

having at least one pre-defined entry point addressable by at least one local client computer;

receiving an input at the remote server from one of the local client computers via the Internet;

automatically addressing one of the web page script entry points based upon the input received at the remote server;

automatically determining a desired security state based upon which entry point is addressed;

automatically passing the determined security state from the remote server to a security state script; and

automatically directing the local client computer, via the security state script, to load replacement frames having the desired security state for each frame of the Internet web page." (emphasis added)

1.3 Rejection of Claims 18-23:

The Office Action rejected independent claim 18 under 35 U.S.C. §103(a) based on the same rationale as that used for the rejection of independent claim 1, as discussed above, with the additional suggestion that "Brown discloses that the dimensions of a substitute document be made according to a specification (see Brown, column 9, lines 55-57)." However, the Applicants respectively suggest that independent claim 18, which claims "computer executable instructions for dynamically generating at least one web page for inclusion in parent web page having at least two frames, and controlling the security state of the parent web page" is patentably distinct from the combination of the cited references in view the preceding discussion, and in further view of the additional discussion provided below.

Specifically, as noted above, the proposed ***Brown / Schneider*** combination ***fails to teach or suggest all the claim limitations***, including for example, the claimed

limitation of "***automatically directing*** the at least one local ***client computer to load replacement frames having the same security state as the customized web page for any existing frames of the parent web page which have a different security state than the customized web page***."

In addition, the Office Action makes no suggestion whatsoever that either of the cited references teaches the claimed limitation of: "*a dynamic web page generation script capable of accepting parameters passed from at least one intermediate page used to call the dynamic web page generation script.*" However, it should be noted that in the rejection of claim 1, the Office Action used the word "intermediate" in suggesting that the "document generator" disclosed by ***Brown*** uses a "determination by a proxy server (see column 3, line 66 to column 4, line 6)" regarding "undesired portions (frames) in a document..." "is further based upon the layout of the ***intermediate document*** (see column 4, lines 42-49)" (emphasis added).

However, in stark contrast to the position advanced by the Office Action, the applicants respectfully suggest that ***Brown*** fails completely to disclose any "intermediate document." In fact, the cited portion of the ***Brown*** reference specifically states:

> "...the controller has a device or mechanism for matching the dimensions of the substitute document portion with the dimensions of the original document portion being replaced, i.e., the undesired original document portion. This provision ensures that the swapped information will be of appropriate size when rendered on the user's screen, thus preserving the page layout which would have been obtained without swapping."

In other words, ***Brown*** is explaining that a mechanism is provided for ensuring that replacement content (i.e., the "substitute document portion") has the same dimensions as the dimensions of the unwanted content that is being replaced. Clearly,

this portion of the disclosure fails completely to disclose any sort of intermediate web page that passes parameters to a "dynamic web page generation script" as disclosed and claimed by the applicants.

Therefore, in view of the preceding discussion, the applicants respectfully suggest that no prima facie case of obviousness has been established in accordance with M.P.E.P. Section 706.02(j) and in accordance with the holdings of *In Re Fine*. This lack of a prima facie showing of obviousness means that the rejected claim 18, and thus dependent claims 19-23 are patentable under 35 U.S.C. §103(a). Therefore, the Applicants respectfully traverse the rejection of claims 18-23, and request reconsideration of the rejection of claims 18-23 under 35 U.S.C. §103(a) over ***Brown*** in view of ***Schneider*** in view of the non-obviousness of the language of claim 18. In particular, claim 18 recites the following novel language:

> "A computer-readable medium having computer executable instructions for dynamically generating at least one web page for inclusion in parent web page having at least two frames, and controlling the security state of the parent web page, said computer executable instructions comprising:
>
> ***a dynamic web page generation script capable of accepting parameters passed from at least one intermediate page used to call the dynamic web page generation script***;
>
> wherein the dynamic web page generation script further comprises at least one encapsulated web-based function which is automatically configured in response to the parameters passed from the intermediate page;
>
> ***dynamically generating at least one customized web page, having a desired security state, in response to the automatic configuration of each encapsulated web-based function***;

transmitting each customized web page from a remote host computer to at least one local client computer via a network;

and

automatically directing the at least one local client computer to load replacement frames having the same security state as the customized web page for any existing frames of the parent web page which have a different security state than the customized web page. (emphasis added)

CONCLUSION

In view of the above, it is respectfully submitted that claims 1-23 are in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of claims 1-23 and to pass this application to issue. Additionally, in an effort to further the prosecution of the subject application, the Applicant kindly invites the Examiner to telephone the Applicant's attorney at (805) 278-8855 if the Examiner has any questions or concerns.

Respectfully submitted,

Mark Watson

Mark A. Watson
Registration No. 41,370
Attorney for Applicants

Lyon & Harr
300 Esplanade Drive, Suite 800
Oxnard, California 93036
(805) 278-8855